

**THOMAS J. FALVEY, COMMISSIONER  
PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE  
PROTECTION  
NDIA  
17 June1998**

• **WAITING FOR DISASTER IS A DANGEROUS STRATEGY**

Earlier this week Steve Mitchell gave you an overview of the work of the President's Commission on Critical Infrastructure Protection and the resultant Presidential Decision Directive 63, or PDD. For the next 30 minutes, I'd like to share some perspectives of infrastructure assurance and how it relates to DOT and the transportation industry.

I'd like to go over some the challenges facing DOT and the transportation industry in implementing infrastructure protection within the transportation sector. First a quick overview of the transportation sector, and a little on how DOD plays into the equation.

Of all our critical infrastructures, transportation is perhaps the most visible from a physical perspective. Through the years and through innumerable incidents, the owners and operators of transportation have learned to deal with the physical threat, from natural disasters to terrorist attacks. However, transportation now depends on information and communication systems we never see. All our modes of transportation, as well as other sectors, are increasingly becoming dependent on GPS. SCADA systems remotely monitor and operate pipelines over thousands of miles of pipe. With the ability to expand highway capacity greatly limited by any number of factors, Intelligent Transportation Systems, or ITS, are increasingly becoming critical to managing highway traffic growth. Ships are tracked into and out of our largest ports by Coast Guard's Vessel Traffic Services, critically dependent on voice communications, radar and television monitoring systems, and computer tracking systems. Our National Airspace System is undergoing the final design phase for replacing our 25 year antiquated system. This new architecture is dependent on open system architectures, GPS, new computer based management systems, and digital communications.

In the past the business of transportation has largely been conducted with paper-based contracts and agreements, orders, letters of credit, invoices, and manifests. Today, however, the business of transportation, along with the world around us, is rapidly adapting to a virtual world. The information technology explosion is generating new ways of doing business. Transportation is becoming an information-based industry critically dependent on data and instantaneous communications. Electronic commerce and electronic data interchange, making just in time delivery the norm rather than the exception, are increasing efficiencies and giving many industries and companies a competitive edge in the global economy. Railroad companies continue to merge, consolidating operations centers and rail lines, moving more and more traffic onto fewer corridors, making these systems more vulnerable to attack. Railroads depend on extensive and interactive databases to track equipment and shipments, ensure proper billing, and ensure effective scheduling for intermodal connections. Computers have

become indispensable and critical to the efficient running of our rail and mass transit systems, for operating our pipelines, and for controlling traffic flows in our cities and on our roads. Yet, at the same time, information system operation and maintenance are being outsourced, highlighted most visibly by the Y2K problem. Extensive dependencies on data bases, Supervisory Control and Data Acquisition (SCADA) and other control systems, and a customer focus allowing computer-based updates on shipments, make these systems more vulnerable to intrusion via the internet and communication lines.

The Commission found that while this nation's transportation system is robust, new information-based systems are creating new vulnerabilities that are not yet fully understood. While the industry has a long history of responding to natural disasters and other threats and keeping our transportation system running, for the most part little consideration is given to the growing vulnerability of our information-based systems. Critical transportation nodes do exist, most of which are largely recognized by the owners and operators — the challenge is how to protect those nodes during a national emergency. Greater government oversight is not the answer. I believe that given the right information, industry will take the necessary steps to protect their critical systems, and thus contribute to the security and the economic well being of the nation. DOT must act as the leader, the facilitator, and take the initiative to get critical information and share it with the owners and operators of our critical transportation infrastructure.

I spoke at a transportation conference this past year, with a major focus on use of the internet to conduct business. Not one mention was made of security considerations. We must realize that today even amateurs have access to the technological tools needed to penetrate systems and cause trouble. The Internet contains hacker sites with simple instructions on how to penetrate systems. The capability to intrude into computer systems increases with a corresponding drop in the computer skills needed to use those tools. System managers are frequently hired without adequate background checks, and in many cases maintenance of information systems are being outsourced with no security controls whatsoever. We've all heard of the Y2K problem facing this country — and I believe this is the greatest of all threats facing this country today—but how much thought is given to where the Y2K solutions are being implemented. The end result is that infrastructures are constantly in danger from people intent on penetrating or disrupting them -- all they need is a personal computer and a modem. The question that our CEO's and CIO's must ask is whether or not we're staying ahead of that trend.

In summarizing some of the findings related to the transportation sector, the Commission found the existing threat dissemination and information sharing process is relatively informal and geared to counterterrorism, not to information based threats. Except for aviation and ports, infrastructure contingency and response plans are non-existent, as are industry security standards and guidelines. Security managers, particularly on the information side, are unable to make a case for action because of a lack of credible data. While we assume the private sector knows its own critical assets, we have no process to identify those facilities that may require protection during a national emergency.

On the Defense side, Department of Defense Planning Guidance (DPG) 2000-2005 just published in April 1998 notes national guidance requires the Department to develop a plan for protecting its own critical infrastructures, implement that plan within two years, and contribute its portion of the National Infrastructure Assurance Plan. To advance the development of an assurance assessment capability, DOD Directive 5160.54 Critical Asset Assurance Program provides a framework to develop the requisite plan and provide a satisfactory level of infrastructure assurance. The Secretary of the Army is the Executive Agent for that program.

The DPG further tasks the services and most of the unified commands, including TRANSCOM, to:

- identify the critical or minimum essential infrastructure required to provide an acceptable level of service;
- develop and implement plans for the assurance of their critical infrastructures; and
- establish standing intelligence collection requirements and a threat baseline.

Just recently DOD, in Joint Vision 2010, adopted "Dominant Maneuver" as a theme, meaning DOD will require rapid movement of materials, troops and supplies to any point on the globe – "just in time delivery" – from fort to foxhole. Any delay or disruption of that system will have serious impact, and therefore, we must ensure our transportation systems are secure.

Recognizing the need to closely cooperate, DOT and TRANSCOM is developing a close working relationship to ensure we leverage each others capabilities in analyzing threats and vulnerabilities to critical transportation assets, and in developing a plan to assure those assets both for national as well as economic security.

The NAS presents a serious challenge to DOT. The Federal government must take the lead in protecting critical infrastructure. The NAS is a highly visible asset that presents a tempting target to the information warriors and hackers around the world. However, the current version of the modernized NAS is vulnerable because of open system architectures, internet connectivity, an absence of backups to critical systems, a risky dependency on GPS, and a sharing of operational and administrative systems.

Speaking of GPS, the current Federal Radionavigation Plan calls for GPS to be the sole radionavigation service by 2010. Nonetheless, we see a general lack of awareness of GPS vulnerabilities, particularly to man-made and natural interference.

These open questions on the vulnerabilities of the NAS and GPS continue to lead us to one basic conclusion:

### **WE MUST ACT NOW TO PROTECT OUR FUTURE**

To do that we must convince our leaders of the future threat without an obvious current threat.

**The threat is largely unknown and undefined in the traditional sense. Technology is largely unavailable to detect intrusions into information systems; we have no idea of how extensive a problem we have. Hacker tools are freely available on the WWW. Thousands of viruses exist. Many critical systems have unauthorized, unprotected external modem connections. Tests have shown even well protected systems can be hacked and penetrated. If a terrorist or nation-state decided to wreck havoc on the US, a kid can be hired for a few thousand dollars to do the work and not leave a trail. Unlimited vulnerabilities with an undefined threat present unparalleled challenges to risk as well as financial managers.**

If this commission ultimately has any impact on securing our critical infrastructures, the Federal Government likely will need to take a strong leadership and coordinating role. Within the transportation sector, DOT must take that role -- not armed with a regulatory solution, but as a coordinator and facilitator, as a leader. Industry and DOT must come together and develop at least a basic contingency plan on how to respond to a threat or an attack on our transportation systems. If DOT can get segments of the transportation industry together to address common threats and vulnerabilities, on a non-adversarial and non-attributional basis, even if DOT stays out of the room, we will be doing a great service to the nation and go a long way to preserving our national security and economy.

#### **GOVERNMENT MUST SET THE EXAMPLE, BUT THE OWNERS AND OPERATORS ARE THE KEY TO SUCCESS**

The increased risk of computer crime has led to the Attorney General's announcement of the start-up of the FBI's National Infrastructure Protection Center well before the final signing of the PDD. Almost concurrently the press reported several cases of criminal hacking into sensitive systems, in particular the "Solar Sunrise" event.

We in DOT support the FBI's jumping our in front of the problem in such an aggressive fashion by establishing the NIPC. We see one of their most critical responsibilities will be rapid and concise reporting of ongoing information-based attacks. Yet, we all know establishment of the center in the FBI will not immediately solve all our computer intrusion problems. The FBI must be given time to establish an effective analysis and dissemination process. Law enforcement agents, historically trained to keep law enforcement sensitive information from public disclosure, must now be trained to share information to protect our critical systems. We, both industry and government, must press the FBI to notify Federal agencies and others of ongoing attacks on computer and other information systems. This highlights the key issue -- how to balance the needs of law enforcement with the overarching need to protect our infrastructures. This issue will present a major national policy challenge in the months and years to come.

We must improve our information sharing and threat dissemination processes. We need to understand who needs what information, develop effective systems and processes to share that information, and ensure that information gets to the individual who needs to

take action. We must routinely test the effectiveness of that system. We must break down the information stovepipes that now exist. And it must be a two way street. Both the private sector and the federal government may be faulted for not sharing information. We must find a way to trust each other.

Information overload also presents a significant challenge. Once we start sharing information as envisioned, how do we process the data, sort out the important data while ensuring we protect it from public disclosure and not compromising law enforcement investigations, and disseminating with sufficient confidence to take perhaps costly countermeasures.

**Until the issue of protecting sensitive information is resolved, we must make this clear to the industry: Do not share any information with the government you would not want on the front page of the Washington Post!.**

Unfortunately, with new technologies comes new vulnerabilities, and our systems have been slow in identifying the need for reducing those vulnerabilities. Organizations may help themselves by requiring assurance provisions when they design and purchase new systems. Beyond that, both the federal government and the industry must identify their critical systems and increase efforts to conduct R&D to protect those systems. Security guidelines or standards must be developed to assist industry and local authorities in developing and protecting their systems from intrusion.

I'd like to review quickly a few key points from PDD-63.

The PDD established lead federal agencies to act as sector coordinator for each of the critical infrastructures. Lead functional agencies, DOD, Justice and FBI, CIA, and State, are also established. A senior level interagency group will coordinate federal government efforts, and a National Infrastructure Assurance Council will provide CEO level advice to the President.

As for DOT, we must work with the transportation sector to identify and establish a sector coordinator who will have the trust of each of six competing modes of transportation. We may have to look at one central location such as an educational institution or an association, or we may have to have one coordinator for each of the six modes. The sector coordinator and the sector liaison official, RADM Bert Kinghorn, must work together to assess vulnerabilities, develop a plan to reduce those vulnerabilities, develop a system to identify and prevent major attacks, and a plan to alert, contain, and rebuff and attack.

We must somehow overcome the natural reluctance of the regulatee trusting the regulator, and vice versa. We must find a way to protect information that is given to the government, not only to protect national security interests, but also the proprietary interests of the company itself.

Education and awareness is the first and perhaps the biggest challenge. How can we convince our leaders of the threat in a time of zero budget growth, either inside or out of the government. And once we make our leaders familiar with the problem, how do we convince the long term government employee or mid-level corporate manager to implement assurance policies that ultimately impact the bottom line with no immediate or obvious payback. If we take no action to invest in assuring the NAS, how will the government ever get the credibility with its own industries.

To protect our critical infrastructures, both government and industry alike must stop thinking solely in terms of terrorism. While we scramble to protect our planes and ships against bombs, we do little or nothing to protect the information systems that could not only compromise safety, but the nation's economic security as well as the competitiveness and perhaps the future of individual corporations.

I'd like to highlight an excellent example of a grass roots effort to improve the security of information infrastructure. In Seattle, an information security manager for a large medical group realized he did not have the tools necessary to do his job. Working with other security managers within the area, including federal, state and local governments and many other corporations, a loose knit organization called the Agora arose. Using largely a virtual network, this group of information security professionals established an extremely effective information sharing network whose sole purpose is to raise the lever of information security among those 100+ members. Once we all recognize the value to our critical systems and business processes, this type of grass roots efforts could form the basis for a national information sharing process that will evolve into a trusted network of security professionals working together to strengthen our nation and its economy. Building on these grass roots efforts, individual agencies can then provide support in areas of threat briefs and warnings, training and awareness programs. Government must be a partner in those efforts.

But we must also be careful. Government must be sure it can protect sensitive corporate information that would normally be releasable under the Freedom of Information Act, or state sunshine laws. Government must also put its own house in order, by securing critical systems such as the National Airspace System and its own information infrastructure.

From the private side, how can the federal government facilitate protection of information systems that are closely linked and critical to the nation, such as the railroad computer systems. Considering their nature, sharing data for operating the nation's rail system, while providing on-line customer service for shippers to locate their product, how do we test and strengthen these systems from penetration. And ultimately what is the government's role. The government can start by inviting play by the private sector and other agencies in DOD infrastructure based exercises.

That concludes my remarks. I'd love to hear any ideas you may have in solving some of these issues, particularly that of the government-private sector coordinator.